REMARKS

Election Requirement

The Patent Office issued a restriction requirement in regard to the present application, wherein the restriction was drawn to Group I (consisting of claim 1), Group II (consisting of claims 2—67), and Group III (consisting of claims 68—87).

During a telephone conference with the Patent Office on March 6, 2002, an election was made with traverse by Applicant to prosecute the invention of Group II, consisting of claims 2—67.

Background

In the Office Action of January 21, 2005, the Patent Office examined claims 2-67.

The specification at page 1, lines 12—20 was objected to as requiring updated cross-reference citation. In response to the objection, Applicant submits herein an amendment to the specification that provides the updated cross-references. Applicant therefore respectively requests that the objection to the specification be withdrawn.

The drawings of the present application were objected to as failing to comply with 37 CFR 1.84(p)(5) because the Patent Office asserts that the drawings include references not mentioned in the description, in particular "items 216 and 281—288 in fig. 2a—b." Applicant respectfully traverses the Patent Office's objection and would direct the attention of the Examiner to pages 11—14 of the specification wherein a full description of the corresponding reference numerals can be found. Applicant is not aware of any references in the drawings that are not also included in the description. Therefore, Applicant respectfully requests that the objection to the drawings be withdrawn.

The pending claims 2-36 were determined to be unpatentable under the judicially created doctrine of obviousness-type double patenting over "claims 1-4 and 1" of U.S. Patent No. 6,820,202, No. 6,820,199 and No. 6,789,189. Further, pending claims 2-67 were determined to be unpatentable under the judicially-created doctrine of obviousness-type double patenting over claim 21 of U.S. Patent Application No. 10/248,623 (note:

since U.S. Patent Application No. 10/248,623 comprise only 20 claims with independent claim 1 as the only independent claim within the claim set, Applicant assumes that the Patent Office's rejection under U.S. Patent Application No. 10/248,623 refers to independent claim 1 and its response herein is made accordingly).

The Patent Office further rejected claims 2-21, 23, 24, and 29-38 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,671,279 issued to Elgamal. Claims 2-67 were further rejected by the Patent Office under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,213,391 issued to Lewis in view of U.S. Patent No. 6,061,799 issued to Eldridge, et al.

Terminal Disclaimer

Before addressing the Section 102 and 103 substantive rejections, Applicant hereby addresses the obviousness-type double patenting rejections.

As suggested by the Patent Examiner, a timely filed Terminal Disclaimer generally may be used to overcome such a rejection for each patent and patent application that is owned by the common assignee of the present patent application and each appropriate patent and patent application.

Terminal Disclaimer for Related Cases

In response to the Final Office Action, Applicant agrees to voluntarily submit and submits herewith a Terminal Disclaimer on the behalf of First Data Corporation that is the 100% owner and common assignee of the present patent application and of the following, related patents and patent application. Specifically, this Terminal Disclaimer is directed to the following patents:

U.S. Patent No. 6,789,189
U.S. Patent No. 6,820,199
U.S. Patent No. 6,820,202

To support the Terminal Disclaimer that has been submitted herewith, Applicant also submits herewith a Statement under 37 CFR 3.73(b) for the present application, the statement confirming the 100% ownership interest in the present application by First Data Corporation. The ownership interest in the patents and patent application cited in the attached Terminal Disclaimer is presently recorded at the U.S. Patent and Trademark Office at reel/frame 013398/0294 for U.S. Patent No. 6,789,189, at reel/frame 012672/0340 for U.S. Patent No. 6,820,199, and at reel/frame 009755/0968 for U.S. Patent No. 6,820,202.

No Terminal Disclaimer for Distinguishable, Patentably Distinct Case

On the other hand, Applicant does not believe that it is appropriate to submit a Terminal Disclaimer for the present application over U.S. Patent Application No. 10/248,623 for the following reasons.

The only, currently-presented independent claim of the present application (claim 2) is directed to a high level account authority digital signature (AADS) system in which a method of operating by a third party a database for accounts, information pertaining to each account being retrievable from the database based on a unique identifier for that account, comprises the steps of (a) first associating by the third party a public key of a respective public-private key pair with each unique account identifier, and thereafter (b) performing entity authentication by the third party with respect to an electronic communication that is received by the third party and that includes both a unique account identifier and a digital signature for a message regarding the account associated with the unique account identifier, the entity authentication consisting of conducting message authentication only using the digital signature received in each electronic communication and the public key associated with the unique account identifier accompanying the digital signature, and without the need for a digital certificate.

In contrast, the one independent claim of U.S. Patent Application No. 10/248,623 is directed to an account-based digital signature (ABDS) system in which an electronic communication is received from a suspect device and based on the security features of

the suspect device, which is maintained in a database in association with the public key of the public-private key of that device, gauging the risk that the digital signature was fraudulently sent (even though the message authenticates) based on such security features. It is respectfully submitted that performing entity authentication consisting of conducting message authentication only using the digital signature received in each electronic communication and the public key associated with the unique account identifier accompanying the digital signature, and without the need for a digital certificate is not obvious in light of and does not itself make obvious a method of using security features of a device, wherein such features are stored in a database and associated with a public key of the device, to enable a recipient of a digitally signed message to gauge the risk that a properly signed and authenticated message may nevertheless not be authentic.

It is respectfully submitted that the Patent Office has failed to make a *prima facie* case of obviousness over the claims of the above-mentioned patent application cited sufficient to warrant or necessitate the filing of a Terminal Disclaimer over this additional reference. There is no suggestion or motivation to modify the reference or combine the reference teachings with any additional teachings. Further, the reference does not teach or suggest all elements of Applicant's claims. Only the disclosure of the present invention makes such a suggestion and it is inappropriate to use such disclosure to support a finding of obviousness between the present invention and the additional cited references.

For the above-stated reasons, the Applicant respectfully submits that the subject matter and specific elements of the claims of the present application are not obvious over the claims of US Patent Application No. 10/248,623. For these reasons, the Applicant declines to submit a Terminal Disclaimer directed to US Patent Application No. 10/248,623. Applicant would further request that the Patent Office contact the undersigned attorney if any further explanations or clarification as to the differences and non-obviousness between the present application and the claims of US Patent Application No. 10/248,623 is required.

Rejections under 35 U.S.C. §§102(b) and 103(a)

Elgamal

The patent to Elgamal appears to describe, generally, a protocol to secure a courier electronic payment system that provides customers, merchants, and banks with a system for credit card payment services. The system, as disclosed, regulates the relationship between a customer, a merchant, and an acquiring bank in order to implement credit card purchases securely over a network.

In regard to the rejection of independent claim 2, the Patent Office cited Elgamal as teaching "a method of operating by a third party (see col. 6, line 67 and col. 7, line 1) a database for accounts, information pertaining to each account being retrievable from the database based on a unique identifier for that account (see col. 6, lines 56—58).

A review of Elgamal finds that the system as described is an electronic payment protocol (col. 3, line 37) involving a relationship between a first party (a Customer **16**), a second party (a Merchant **18**) and a third party (an Acquiring Bank **20**). A Merchant application **18** is implemented within the system, wherein the Merchant application **18** comprises "a database of all open transactions" (col. 6, line 56) with Customers **16**, the database further comprising "corresponding Transaction Ids and AuthIDs with customer information (col. 6, lines 56—58)."

Nowhere is it taught in Elgamal that a third party (in this instance the Acquiring Bank **20**) operates a database for accounts, wherein information pertaining to each account [is] retrievable from the database based on a unique identifier for that account. In contrast, Elgamal describes a three party system wherein a second party (Merchant) to a transaction possesses a database of current transactions with first parties (Customers).

Elgamal was further cited for teaching the step of "first associating by the third party a public key of a respective public-private key pair with each unique account identifier (see col. 6, lines 56—58 and 66; col. 7, lines 1 and 52—56 and col. 10, lines

20—23)." In this instance Elgamal describes that the third party (the Acquiring Bank 20) assigns a Merchant ID to the Merchant (the second party), wherein the Merchant ID is "a unique number for each merchant assigned by the acquirer signing up the merchant (col. 7, lines 52—53)." This description is in direct contrast to the Patent Office's position that the Merchant is the third party that associates a public key of a respective public-private key pair with each unique account.

Further, the PI (payment information) that is cited by the Patent Office at (col. 10, lines 20—23) is actually transaction payment information that is transmitted from the second party (the Merchant) to the true third party entity (the Acquiring Bank) using the Acquiring Bank's public key and not a public key belonging to the Merchant. The systematic configuration as set forth by the Patent Office does not technically or structurally make sense or comprise any spirit of the intended invention as described by Elgamal. Nowhere is it taught in Elgamal the step of associating by a third party a public key of a respective public-private key pair with each unique account identifier.

Thus, nowhere is it taught, described, or disclosed in Elgamal a method of operating by a third party a database for accounts, information pertaining to each account being retrievable from the database based on a unique identifier for that account, wherein the method comprises the step of first associating by the third party a public key of a respective public-private key pair with each unique account identifier.

Further, in contrast to the present invention, the entire authentication and non-repudiation scheme described in Elgamal relies upon use of conventional digital certificates issued by authorized certification authorities to ensure the integrity and validity of such keys so that they can be relied upon by other parties (see, e.g., col. 6, lines 43—67 through col. 8, lines 1—45 and cols. 15-20 generally). The use of digital certificates, as described by Elgamal, is conventional and has already described in the background of the invention section of the present application.

As opposed to this "certificate authority digital signature" (CADS) system, which is contrasted with the present invention in the background of the invention section, the

present invention relates to an "account authority digital signature" (AADS) system in which an account authority, with which an account holder actually maintains an account, first associates a public key of the account holder with an account having a unique account identifier, and thereafter authenticates a digitally-signed message from the account holder using the public key associated by the account authority for the account referenced in the digitally-signed message and without need of a digital certificate. In the AADS system, no digital certificates need be sent with the digitally signed message and, consequently, no certificate issuing authority (i.e., certification authority) need be consulted regarding the continued validity of a digital certificate or of the public-private key pair.

Therefore, since Elgamal fails to teach each and every element of the limitations of claim 2, Applicant respectfully requests that the Patent Office withdraw the rejection of claim 2 under 35 U.S.C.§102(b).

It is further respectfully submitted that since the independent claim 2 is allowable and since each dependent claim merely adds further limitations or elements to those independent claims, it is respectfully submitted that all of the currently pending claims 2—67 are allowable over this reference of record.

Lewis

Lewis was cited as a primary reference in the rejection of claims 2—67 under 35 U.S.C. §103(a). Lewis appears to describe a portable device for use in confirming personal identification of the user of the device based upon distinctive characteristics of the user. As shown in FIG. 1 of Lewis, such device 1 stores or pre-stores user profiles in (database) storage 6. Such user profiles include distinctive characteristics of the user, such as digitized biometric information. Suspect user identification information is input into the device at input 12,14. If necessary, such suspect user identification information is digitized and then compared with the pre-stored user profiles from storage 6. If there is a match, a positive ID signal is generated and sent to output 10. If there is not a match, a

negative ID signal is generated and sent to output 10. As a back-up, the digitized suspect user identification information 4 is also converted into a suitable code by means of code generator 5 and such code is sent to output 11. This generated code is useful as a "secondary, or alternative method of determining identification and authorization." (col. 9, ll. 3-5). However, it is necessary for the recipient of the signal from output 11 to have access to or prior knowledge of the user's profile and the technique or algorithm used by code generator 6 in order to determine independently whether there is a match. FIG. 2 appears to describe a similar but slightly different embodiment compared to FIG. 1. In FIG. 2, the signals at outputs 30, 29 are encrypted to prevent interception of such information as it is transmitted to the recipient.

Nothing in Lewis teaches, discloses, or suggests a method of operating by a third party a database for accounts, wherein information pertaining to each account is retrievable from the database based on a unique identifier for that account, comprising the steps of (a) first associating by the third party a public key of a respective public-private key pair with each unique account identifier, and thereafter (b) performing entity authentication by the third party with respect to an electronic communication that is received by the third party and that includes both a unique account identifier and a digital signature for a message regarding the account associated with the unique account identifier, the entity authentication consisting of conducting message authentication only using the digital signature received in each electronic communication and the public key associated with the unique account identifier accompanying the digital signature, and without the need for a digital certificate.

It is respectfully submitted that Lewis, which is directed to a portable device that contains information about a user of the device and which authenticates the user of the device by comparing information input into the device with information pre-stored in the device has limited-to-no relevance and applicability to the method of the present invention, as set forth in claim 2.

Eldridge

The second, supporting reference relied upon by the Patent Office, Eldridge, appears to describe a dual shared-secret authentication system useful for authenticating a client process to a server process. The client process uses a portable medium or device to store both current and past passwords of the client process. Each password (current and past) on the portable medium has associated with it a key (e.g., a public-private key pair or just a public key) and a key ID wherein the key and corresponding key ID are both derived from the client-chosen password. The client process (portable medium/device) also has an associated client ID for identifying itself to the server process. The server process also possesses the same key-key ID pairs, as well as the associated client ID (see, e.g., col. 7, ll. 64-col. 8, ll. 12).

To authenticate, as shown in FIG. 5 of Eldridge (col. 7), the client process first provides its client ID to the server process (col. 7, ll. 22-24). The server process then retrieves the associated key ID and provides it to the client process (col. 7, ll. 24-30). The client process uses this key ID to identify the corresponding key and provides such key back to the server process (col. 7, ll. 30-43). The server process then generates a new key ID from the key received from the client process and compares this new key ID with the key ID it originally sent. If these match, then the client process is authenticated (col. 7, ll. 43-48). In an alternative, more simplistic, and less reliable embodiment, as shown in FIG. 7 of Eldridge (col. 9), the server process extracts both the client ID and key ID from the portable medium (col. 9, ll. 40-50). The server process uses the client ID to identify the corresponding key IDs previously stored in its own database. If there is a match, then the client process is authenticated.

It is also respectfully submitted that Eldridge does not assist in making Lewis a more relevant reference. Further, nothing in Eldridge teaches, discloses, or suggests a method of operating by a third party a database for accounts, wherein information pertaining to each account is retrievable from the database based on a unique identifier for that account, comprising the steps of (a) first associating by the third party a public key of a

respective public-private key pair with each unique account identifier, and thereafter (b) performing entity authentication by the third party with respect to an electronic communication that is received by the third party and that includes both a unique account identifier and a digital signature for a message regarding the account associated with the unique account identifier, the entity authentication consisting of conducting message authentication only using the digital signature received in each electronic communication and the public key associated with the unique account identifier accompanying the digital signature, and without the need for a digital certificate.

Combination of Cited Art

The Patent Office has relied upon Lewis in view of Eldridge; however, the Patent Office has failed to show how Lewis and Eldridge teach singly or in combination the performance of entity authentication by a third party with respect to an electronic communication that is received by the third party and that includes both a unique account identifier and a digital signature for a message regarding the account associated with the unique account identifier. Nor does Lewis or Eldridge in combination teach that the entity authentication consists of conducting message authentication using only the digital signature that has been received in each electronic communication and the public key that is associated with the unique account identifier accompanying the digital signature.

Applicant asserts that the Patent Office has used impermissible hindsight in the construction of the rejection of independent claim 2 of the present application. The U.S. Court of Appeals for the Federal Circuit (the "Federal Circuit") restated the legal test applicable to rejections under 35 U.S.C. § 103(a) (*In re Rouffet*, 47 USPQ2d 1453 (Fed. Cir., July 15, 1998)). The Court stated:

> [V]irtually all [inventions] are combinations of old elements. Therefore an Examiner may often find every element of a claimed invention in the prior art. Furthermore, rejecting patents solely by finding prior art corollaries for the claimed elements would permit an Examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to

> determine patentability." To prevent the use of hind sight based on the invention to defeat patentability of the invention, this court requires the Examiner to show a motivation to combine the references that create the case of obviousness. The Board [of Appeals] did not, however, explain what specific understanding or technological principle within the knowledge of one of ordinary skill in the art would have suggested the combination. Instead, the Board merely invoked the high level of skill in the field of the art. If such a rote indication could suffice to supply a motivation to combine, the more sophisticated scientific fields would rarely, if ever, experience a patentable technical advance. Instead, in complex scientific fields, the Board could routinely identify the prior art elements in an application, invoke the lofty level of skill, and rest its case for rejection. To counter this potential weakness in the obviousness construct **the suggestion to combine requirements stands as a critical safeguard against hindsight analysis and rote application of the legal test for obviousness.**
>
> *In re Rouffet*, 47 USPQ2d 1457-58 (Fed. Cir., July 15, 1998) (citations omitted, emphasis added).

The invention claimed in the present application, as set forth in independent claim 2 is not rendered obvious by the above reference. To the extent the Patent Office is inclined to combine disparate pieces of the above reference in an attempt to craft the present invention, it serves as a reminder that in order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art references or combination of references must teach or suggest all the claim limitations. Most importantly, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP §2142.

Therefore, in view of the above remarks the Applicant respectfully request that the rejection of independent claim 2 be withdrawn under 35 U.S.C. 103(a) based on Lewis and Eldridge.

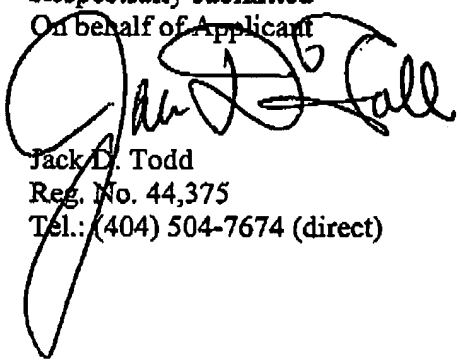
Dependent Claims

Further, because the only pending independent claim 2 is believed to stand in condition for allowance, Applicant submits that the dependent claims 3—67 similarly are allowable. Applicant nevertheless respectfully submits that each of these dependent claims is allowable based on the additional recitation of such dependent claim, and Applicant requests consideration thereof as necessary. Applicant further does not acquiesce in the rejections of these dependent claims, but Applicant does not *per se* address each such rejection, as Applicant believes such rejections are moot in view of the foregoing remarks.

Conclusion

In view of the foregoing amendments and remarks, the enclosed terminal disclaimers, and associated fees, Applicant submits that the present claims now stand in condition for allowance, and Applicant respectfully requests notice of the same. It furthermore is respectfully requested that the Examiner contact the undersigned if any further action is deemed necessary in order to gain allowance of the present application, and if such further action may be accomplished through action by the Examiner.

Respectfully submitted
On behalf of Applicant



Jack D. Todd
Reg. No. 44,375
Tel.: (404) 504-7674 (direct)

MORRIS, MANNING & MARTIN, LLP

3343 Peachtree Road, N.E.
1600 Atlanta Financial Center
Atlanta, Georgia 30326
(404) 233-7000
Customer No. 24728